Zechariah Copeland, 612-380-3416 LinkedIn.: www.linkedin.com/in/zechariah-copeland-b3b4b1199

Github: https://github.com/zechariahcopelan

Website:

Summary

Proven leader with 10+ years securing and optimizing mission-critical infrastructure across enterprise and academic environments. Expert at incident response, system hardening, and root cause analysis that drives 99.9% uptime and operational resilience. Now advancing into Software Engineering, Cloud Architecture, and AI/ML, blending deep infrastructure expertise with emerging tech skills in Python, AWS/Azure, and machine learning pipelines. Recognized for translating complex technical challenges into actionable solutions, reducing downtime, and safeguarding assets in high-pressure, 24/7 operations.

TECHNICAL SKILLS *

Programming Languages: SQL (Intermediate), Python (Beginner/Learning), JavaScript (Beginner/Learning) * **AI/ML Concepts:** Machine Learning (Beginner/Learning), Artificial Intelligence (Beginner/Learning), Deep Learning (Beginner/Learning), Natural Language Processing (Beginner/Learning) * **Data & Analytics:** Data Analysis, Log Analysis, Root Cause Analysis, Data Structures (Beginner/Learning), Algorithms (Beginner/Learning) * **Cloud & DevOps:** Cloud Computing Fundamentals (Beginner/Learning - e.g., AWS/Azure/GCP), Git (Beginner/Learning), Linux (Intermediate), Containerization (Beginner/Learning - e.g., Docker) * **Systems & Operations:** Network Monitoring, Incident Management, Troubleshooting, System Administration (Windows/Linux), IT Operations, Service Continuity, Process Optimization * **Tools & Platforms:** HP OpenView, Tivoli Workload Scheduler, Cherwell, Pandas, NumPy, Scikit-learn

Network Operations Center Tech 1

University of Wisconsin-Madison, Full-time September 2015- Present Minneapolis, MN

Monitored and optimized a 1,500+ server enterprise infrastructure across multiple data centers, ensuring 24/7 uptime, high availability, and rapid incident response.

Diagnosed and resolved critical production issues in Gigabit Ethernet and mainframe environments through in-depth root cause analysis, proactive alerting, and incident containment.

Leveraged enterprise monitoring and automation tools (HP OpenView, Tivoli Workload Scheduler, Cherwell) to manage incident queues, automate batch processes, and maintain SLA compliance.

Performed forensic-level investigations into recurring job failures, integrating log analysis, network packet inspection, and system performance metrics to restore operations with minimal downtime.

Enforced security and compliance controls aligned with NIST and ISO 27001 standards, strengthening the organization’s posture against vulnerabilities and unauthorized access.

Partnered with cross-functional teams to identify threat patterns, eliminate single points of failure, and implement system hardening measures, reducing repeat incidents by 43%.

Skills: Incident Response · Intrusion Detection & Prevention Systems (IDS/IPS) · SIEM Tools & Log Analysis· Security Hardening (Linux & Windows) Fundamentals · Network Monitoring & Analysis · Log

Analysis & Root Cause Investigation ·Linux/Windows Security Fundamentals · Cloud Security Fundamentals (AWS/Azure) Vulnerability Assessment & Management · Threat Intelligence & Indicators of Compromise (IOCs) · TCP/IP, DNS, VPN & Firewall Configuration · Security Policies, Procedures, and Best Practices (e.g., NIST, ISO 27001)

ATOC Analyst

Asurion, Fulltime October 2013- August 2015

Served as the first line of defense for all company-wide technical issues across software, hardware, network, and database layers, safeguarding a global infrastructure of 10,000+ endpoints.

Monitored and escalated infrastructure threats using enterprise tools, preventing 95% of potential outages before they impacted business operations.

Analyzed system logs and SQL databases to pinpoint root causes, improving incident resolution speed by 38% and reducing average downtime by 27%.

Delivered Tier 2 Windows desktop and server support, including enterprise deployments, OS hardening, and remote troubleshooting, achieving a 90%+ first-contact resolution rate.

Collaborated with cross-functional teams (network, application, and security) to resolve high-priority incidents, cutting incident recurrence by 41% through targeted fixes and knowledge base optimization.

Skills: Incident Response · Intrusion Detection & Prevention Systems (IDS/IPS) · Linux/Windows Security Fundamentals · Network Monitoring & Analysis · Log Analysis & Root Cause InvestigationSkills: Incident Response · Intrusion Detection & Prevention Systems (IDS/IPS) · Linux/Windows Security Fundamentals · Network Monitoring & Analysis · Log Analysis & Root Cause Investigation

Technical Analyst

Dell Technologies, Full-time August 2011-September 2012 Nashville, TN

Provided Tier 1 & Tier 2 enterprise support for Boeing users in a high-security, multi-time zone environment, resolving software, OS, and network connectivity issues with a first-call resolution rate of 87%.

Administered and maintained Active Directory accounts, group policies, and permissions while supporting Citrix environments and custom application deployments.

Leveraged HP Service Manager to log, escalate, and resolve incidents in strict alignment with SLA targets, achieving 99% on-time closure compliance.

Diagnosed and recovered from backup failures, VPN access disruptions, and application errors, restoring system availability 25% faster than baseline response times.

Implemented temporary workarounds during escalations, ensuring continuous productivity and minimizing operational impact across Boeing’s user base.

Skills: Log Analysis & Root Cause Investigation

Degrees:

The University of Tennessee-Martin May 2011

B.S.B.A. in Information Systems Minor: Computer Science

The University of Colorado-Boulder May 2027

Master of Science in Electrical and Computer Engineering GPA:3.5/4.0

Certifications:

Google Cyber Security Certification Issued April 2025